Robert C. Schubert (No. 62684)
Amber L. Schubert (No. 278696)
**SCHUBERT JONCKHEER & KOLBE LLP**
2001 Union. St., Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

*Counsel for Plaintiffs*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO / OAKLAND DIVISION**

Darren Van Antwerp and Bradley Tanzman, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

Patelco Credit Union,

Defendant.

Case No. 3:24-cv-4226

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Upon personal knowledge as to their own acts, and based upon their investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiffs Darren Van Antwerp and Bradley Tanzman, on behalf of themselves and all others similarly situated, allege as follows:

## SUMMARY OF THE ACTION

1. Plaintiffs bring this class action against Patelco Credit Union ("Patelco") for its failure to adequately secure and safeguard their and at least 450,000 other individuals' personally identifying information ("PII").

2. Defendant Patelco is "one of the largest credit unions in the nation" and advertises "$9 billion in assets and over 450,000 members nationwide[.]"[1]

3. In the course of providing services to its members, customers provided their PII, including names, dates of birth, addresses, Social Security numbers, driver's license numbers, and financial account information. Patelco owes these individuals a duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute and common law, at all relevant times, Patelco utilized deficient data security practices, allowing its members' sensitive and private data to fall into the hands of malicious actors.

4. On June 29, 2024, Patelco experienced a ransomware attack (the "Data Breach").[2] In this type of cyber-attack, hackers gain access to a company's computer systems, block access, and then demand a ransom payment to restore its systems and return stolen data.

5. As a result, Patelco shut down some of its day-to-day banking systems, including online banking, its mobile app, and its call center. Accordingly, important services, such as transfers (including Zelle), direct deposit, balance inquiries, and payments became unavailable. It also limited debit and credit card transactions.[3]

---

[1] Who We Are, PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited July 11, 2024).

[2] Security Incident Updates & Information Center, PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited July 11, 2024).

[3] *Id.*

6. Although the perpetrators have not identified themselves, ransomware attacks typically also involve data theft to be used in the extortion phase, which likely involves the sensitive personal and financial information on hundreds of thousands of Patelco members.

7. The Data Breach was directly and proximately caused by Patelco's failure to implement reasonable and industry standard data security practices necessary to protect its systems from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII and PHI of at least 450,000 individuals is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiffs and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes. Moreover, Plaintiffs and Class Members have lost the inherent value of their private data.

8. By aggregating information obtained from the Data Breach with other sources, or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names, birth dates, Social Security numbers, and addresses to open new financial accounts, incur credit charges, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

9. Despite the Data Brach being first detected on June 29, 2024, Patelco has failed to disclose what customer data was disclosed to cybercriminals, and it has not directly notified its members as to what data was stolen. These failures exacerbate the damages and risks to Class Members in violation of California. The notices that Patelco has posted on its website also obscure the nature of the cyberattack and threat it posed—failing to adequately inform Plaintiffs and Class Members how many people were impacted, how the cybercriminal remotely accessed its systems, whether the exfiltrated information was encrypted or anonymized, why it has not directly notified

victims, or what specific remedial steps it has taken to safeguard PII within its systems and networks (or otherwise purge unnecessary information) to prevent further cyberattacks going forward.

10. Plaintiffs Van Antwerp and Tanzman are Patelco members and Data Breach victims, each of whom has experienced severe harms from the loss of access to Patelco's critical banking systems and the Breach of their PII.

11. Plaintiffs, on behalf of themselves and all others similarly situated, herein allege claims for negligence, unjust enrichment or quasi-contract, invasion of privacy, violation of California's Consumer Privacy Act (CAL. CIV. CODE §§ 1798.100, *et seq.*), violation of California's Customer Records Act (CAL. CIV. CODE §§ 1798.80, *et seq.*), violation of California's Unfair Competition Law (CAL. BUS. & PROF. CODE §§ 17200, *et seq.*), and declaratory and injunctive relief. Plaintiffs, on behalf of themselves and the Class, seek: (i) actual damages, economic damages, statutory damages, and nominal damages; (ii) punitive damages; (iii) fees and costs of litigation; (iv) injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII in Defendant's custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and to provide long-term identity theft protective services to Plaintiffs and Class Members; and (v) such other relief as the Court deems just and proper.

## PARTIES

### A. Plaintiffs

12. Plaintiff Darren Van Antwerp is a resident of Rocklin, California and a citizen of California.

13. Plaintiff Bradley Tanzman is a resident of San Francisco, California and a citizen of California.

### B. Defendant

14. Defendant Patelco Credit Union is a California nonprofit corporation headquartered in Dublin, California.

## JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one member of the putative Class, as defined

below, is a citizen of a state other than that of Defendant, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in Dublin, California and regularly conducts business in California, and has sufficient minimum contacts in California, such as to not offend notions of fair play and substantial justice.

17. Venue in this District is proper under 28 U.S.C. § 1391 because Defendant resides in this District, and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting or storing the PII of Plaintiffs and the putative Class Members. Additionally, Plaintiff Tanzman resides in this District.

18. Divisional Assignment: This action arises in Alameda County, in that a substantial part of the events which give rise to the claims asserted herein occurred in Alameda County, where Defendant is headquartered and located. Additionally, Plaintiff Tanzman resides in San Francisco County. Pursuant to L.R. 3-2(d), all civil actions that arise in Alameda County and San Francisco County shall be assigned to the San Francisco or Oakland Division.

## FACTUAL BACKGROUND

### A. Patelco Collected and Stored Its Members' Private Information.

19. Patelco is "a full-service, not-for-profit financial cooperative dedicated to helping our members and communities prosper."[4] It offers a wide range of financial services, including checking and savings accounts, loans, credit cards, investment services, and insurance plans.

20. Patelco is "one of the largest credit unions in the nation" with "$9 billion in assets and over 450,000 members nationwide."[5] It has 37 branches in the San Francisco Bay Area, Sacramento, and San Jose.[6]

---

[4] Who We Are, PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited July 11, 2024).

[5] *Id.*

[6] Bill Toulas, *Patelco shuts down banking systems following ransomware attack*, BLEEPING COMPUTER (July 2, 2024), https://www.bleepingcomputer.com/news/security/patelco-shuts-down-banking-systems-following-ransomware-attack/.

21. As a condition of receiving its services, Defendant requires that its members, including Plaintiffs and Class Members, entrust it with sensitive personal information, including names, dates of birth, addresses, Social Security numbers, driver's license numbers, and financial account information.. Defendant collected and maintained Plaintiffs' and the Class's PII in its computer systems, servers, and networks.

22. In collecting and maintaining Plaintiffs' and the Class's PII, Defendant implicitly agreed that it would protect and safeguard that PII by complying with state and federal laws and regulations and applicable industry standards. Defendant was in possession of Plaintiffs' and the Class's PII before, during, and after the Data Breach.

23. Under state and federal law, businesses like Defendant have duties to protect its current and former customers' PII and to notify them about breaches.

24. Defendant recognizes these duties, declaring in its "Privacy Policy"[7] that:

a. "Your privacy is very important to us."

b. "At Patelco, we respect your right to privacy and understand the importance of maintaining the security of your personal information."

c. "This is another way we are looking out for your financial wellbeing."

d. The security of your personal and financial information is our highest priority."

25. Likewise, in its "Federal Privacy Notice,"[8] Defendant provides that that:

a. "Financial companies choose how they share your personal information."

b. "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law."

c. "These measures include computer safeguards and secured files and buildings. Credit Union staff, management and volunteers are trained to keep consumer information strictly confidential."

[7] Privacy Policy, PATELCO CREDIT UNION (March 20, 2023), https://www.patelco.org/privacy.

[8] Federal Privacy Notice, PATELCO CREDIT UNION (March 20, 2023), https://www.patelco.org/wp-content/uploads/2023/05/Federal-Privacy-Notice.pdf.

26. Despite these strong proclaimed proactive policies and approaches to data security and privacy for its members, Defendant failed to adequately secure and safeguard its own systems and networks from a foreseeable and preventable cyberattack. This conduct proximately resulted in the Data Breach and significant harm to Plaintiffs and the Class.

**B. Patelco Shuts Down Its Systems After a Ransomware Attack and Data Breach.**

27. On June 29, 2024, Patelco experienced a ransomware attack, in which cybercriminals used malware to infiltrate its computer systems and encrypted them, then demanded a ransom to unlock them.

28. At the time, it stated, “"Unfortunately, this incident has required us to proactively shut down some of our day-to-day banking systems in order to contain and remediate the issue.”[9]

29. As a result, Patelco shut down online banking for its members, rendering them unable to access their accounts for basic activity like viewing their balances, making electronic transfers. and scheduling new online bill payments. Services including online banking, mobile apps, monthly statements, Zelle transactions, balance inquiries, new or edited bill payments, and check cashing were offline and unavailable.[10]

30. The shutdown of these critical systems has caused Plaintiffs and Class Members enormous harm, including bounced payments and late-payment and overdraft fees. The inability of Plaintiffs and Class Members to access their online banking systems has left them unable to manage their financial lives, and as a result, these outages may negatively affect their credit scores.

31. Patelco has provided little information about who was responsible for the attack, how much was demanded as ransom, and whether it paid the ransom. A Patelco spokesperson told the San Francisco Chronicle that she was unable to provide further information about the incident, saying only that Patelco was “committed to supporting our members.”[11]

---

[9] Security Incident Updates & Information Center, PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited July 11, 2024).

[10] *Id.*

[11] Jessica Flores, *Massive Patelco cyberattack is still affecting half a million people. Here’s how to protect yourself*, SAN FRANCISCO CHRONICLE (July 12, 2024), https://www.sfchronicle.com/bayarea/article/patelco-lawsuits-struggling-to-recover-cyberattack-19569709.php.

32. Patelco has also not commented on whether the hackers accessed and downloaded Plaintiffs and Class Members private information. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

33. On information and belief, however, Plaintiffs' and Class Members' PII was exposed to cybercriminals. This PII likely includes at least names, dates of birth, addresses, Social Security numbers, driver's license numbers, and financial account information.

34. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals defeated the relevant data security systems and gained actual access to sensitive data. Indeed, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[12]

35. Thus, on information and belief, Plaintiffs' and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

36. Despite Defendant's duties and commitments to safeguard sensitive and private information, Defendant failed to follow industry-standard practices in securing Plaintiffs' and the Class Members' PII, as evidenced by the Data Breach.

37. In response to the Data Breach, on June 30, 2024, Patelco stated, its "teams are working around the clock with top-tier cybersecurity experts to assess the situation and to restore service to you."[13] On July 1, 2024, it stated that it had " engaged a leading third-party cybersecurity forensic firm to help [it] to investigate and recover as soon as possible."[14]

38. On July 3, 2024, Patelco stated that its "cyber security specialists have validated and greenlighted [its] core systems – your money is safe and secure."[15]

---

[12] Brenda R. Sharton, Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for- sale-on-the-dark-web-should-you-buy-it-back.

[13] Security Incident Updates & Information Center, PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited July 11, 2024).

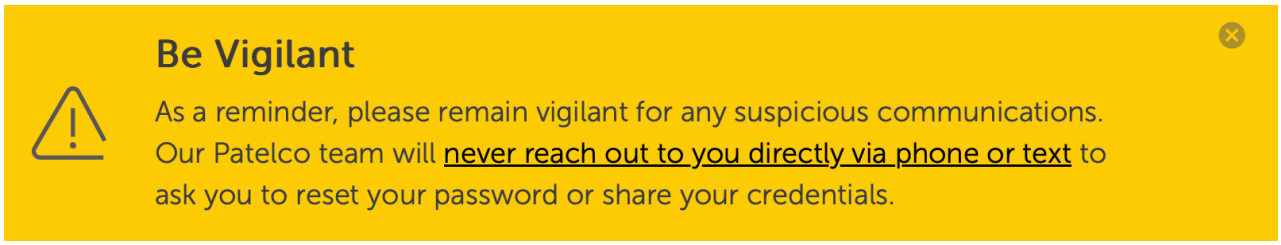
[14] *Id.*

[15] *Id.*

39. On July 13, 2024, Patelco CEO Erin Mendez wrote that "we have meticulously examined and bolstered our environment in order to bring our systems back online. Cybersecurity defense is a constantly moving target, particularly for financial services institutions, which are often targets for these kinds of attacks. We remain committed to making strategic investments in the advanced tools, teams, and partners that help keep us safe."[16]

40. Although Patelco has failed to expand on what these "strategic investments" to bolster the company's cybersecurity entail, such policies and practices clearly should have been in place and fully operational *before* the Data Breach.

41. Through its public communications, Patelco has also recognized the actual imminent harm and injury that flowed from the Data Breach. In a bright yellow banner at the top of every page of its website, it warns its members to "Be Vigilant," reminding its members to "please remain vigilant for any suspicious communications."[17]




42. Indeed, the Data Breach involves PII that is difficult or even impossible to change, such as Social Security numbers and dates of birth. Further, the Data Breach exposed nonpublic, highly private information, which is disturbing harm in and of itself. Even with complimentary short-term identity monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII remains very high. The fraudulent activity resulting from the Data Breach may not come to light for years.

### C. The Financial Industry Is Increasingly Susceptible to Data Breaches, Giving Defendant Notice That It Was a Likely Cyberattack Target.

43. At all relevant times, Defendant knew, or should have known, that the PII it was entrusted with was a target for malicious actors. Defendant knew this given the unique type and the

[16] *Id.*
[17] *Id.*

significant volume of data on its networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

44. As custodian of Plaintiffs' and Class Members' PII, Defendant knew or should have known the importance of protecting their PII, and of the foreseeable consequences and harms to such persons if any data breach occurred.

45. Defendant's security obligations were especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting businesses and other organizations like Defendant, which store and maintain large volumes of PII.

46. Indeed, Patelco's own CEO, Eric Mendez, admitted after the Data Breach, "Cybersecurity defense is a constantly moving target, ***particularly for financial services institutions, which are often targets for these kinds of attacks.***"[18]

47. Patelco, in particular, was put on notice by previous cyberattacks on its computer systems. On or around September 23, 2023, it notified 181,507 members that their personal and baking information was exposed by one of its vendors.[19]

48. In that breach, Patelco disclosed that Progress Software Corporation previously announced a vulnerability in its MOVEit Transfer application used by Patelco's vendor, Sovos, which the credit union utilized to deliver services associated with some member accounts.[20] A well-known Russian ransomware cybergang, Clop, began exploiting this vulnerability since late May and early June 2023 and hacked 2,773 organizations—including credit unions and banks—and 95.7 million individuals.[21]

49. The MOVEit data breach affected numerous credit unions and other financial institutions, including Chevron Federal Credit Union, Franklin Mint Federal Credit Union, TruStage Financial Group, TD Ameritrade, Charles Schwab, Genworth Financial, Fidelity Investments

[18] *Id.* (emphasis added)

[19] Peter Strozniak, *Patelco CU Reported Data Breach in 2023, Affected 181,000 Members*, CREDIT UNION TIMES (July 12, 2024), https://www.cutimes.com/2024/07/12/patelco-cu-reported-data-breach-in-2023-affected-181000-members/?slreturn=20240714-25056.

[20] *Id.*

[21] *Id.*

Institutional Operations, Bank of America, Union Bank and Trust Company, Umpqua Bank, Midfirst Bank, Valley National Bank, Cadence Bank, the Bank of Canton, Flagstar Bank, Community Trust Bank, Primis Bank, M&T Bank, and Wayne Bank.[22]

50. Largescale cyberattacks are increasingly common and well-publicized. The rate of global weekly cyberattacks rose by 7% in the first quarter of 2023 compared to the same period in 2022.[23] And organizations faced an average of 1,248 attacks a week.[24]

51. With the surging number of such attacks targeting financial services firms, Defendant knew or should have known that it was at high risk of cyberattack and should have taken additional and stronger precautions and preemptive measures.

### D. Defendant Breached Its Duties to Plaintiffs and Class Members and Failed to Comply with Regulatory Requirements and Industry Practices.

52. Because Defendant was entrusted with such PII at all relevant times, Defendant owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to its networks and systems. Defendant also owed a duty to safeguard PII because it was on notice that it was handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, Defendant knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

53. Security standards commonly accepted among businesses that store PII include, without limitation:

i. Maintaining a secure firewall configuration;

---

[22] *Id.*

[23] Sam Skolnik, Sky Witley, and Olivia Cohen, *Law Firm Cyberattacks Grow, Putting Operations in Legal Peril* (July 7, 2023), BLOOMBERG LAW, https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril.

[24] *Id.*

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

iv. Monitoring for suspicious or irregular activity by know users;

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII;

viii. Monitoring for server requests from VPNs; and

ix. Monitoring for server requests for Tor exit nodes.

54. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[25] and protection of PII which includes basic security standards applicable to all types of businesses.[26]

55. The FTC recommends that businesses:

i. Identify all connections to the computers where you store sensitive information.

ii. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

iii. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

[25] Start with Security: A Guide for Business, FTC (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[26] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

v. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

vi. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

vii. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

viii. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

ix. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

56. As described further below, Defendant owed a duty to safeguard PII under several statutes, including the Federal Trade Commission Act ("FTC Act"), to ensure that all information it received, maintained, and stored was secure. The FTC Act was enacted to protect Plaintiffs and the Class Members from the type of conduct in which Defendant engaged, and the resulting harms Defendant proximately caused Plaintiffs and the Class Members. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiffs and Class Members.

57. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII by failing to implement and maintain adequate data security measures to safeguard

Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII no longer necessary for its provision of legal services to its clients, allowing unmonitored and unrestricted access to unsecured PII, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Member's confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act.

58. Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, servers, and networks, the Data Breach would not have occurred.

59. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members.

**E. The Experiences of Plaintiffs Van Antwerp and Tanzman**

60. Plaintiff Van Antwerp has been a Patelco member since 2012. Plaintiff Tanzman has been a Patelco member since the 1990s, and after leaving the credit union, returned as a member in approximately 2015.

61. As a condition of becoming customers of Patelco, Van Antwerp and Tanzman were required to provide their PII to defendant, including but not limited to their names, dates of birth, addresses, contact information, and Social Security numbers.

62. At the time of the Data Breach, on or before June 29, 2024, Defendant retained Van Antwerp's and Tanzman's PII in its computer systems.

63. Van Antwerp and Tanzman are very careful about sharing their sensitive PII. They store any physical or electronic documents containing their PII in safe and secure locations. They

would not have entrusted their PII to Defendant had they known of Defendant's lax data security policies.

64. As a proximate result of the Data Breach, Van Antwerp and his business have suffered from not having access to his financial accounts and online banking services. He has had to borrow money for rent his business activities, incurring interest he otherwise would not have paid but for the Data Breach. Van Antwerp has concerns for his personal financial security as a result of the Data Breach given the highly personal nature of PII exposed.

65. As a proximate result of the Data Breach, Tanzman has suffered from not having access to his financial accounts and online banking services. Tanzman uses the Patelco mobile app to lock and unlock his ATM debit card. When the Data Breach occurred, Patelco shut down its app and online banking services, leaving Tanzman with no method to unlock his debit card. Thus, Tanzman was forced to wait in line at Patelco branch offices each day to withdraw cash. For sixteen straight days, Tanzman was forced to visit Patelco branch offices and wait in long lines to withdraw cash. During those visits, Patelco employees recorded his transactions on paper because the company's computer systems were inaccessible. As a result, Tanzman's account balances do not accurately reflect the transactions he made in branch offices.

66. Moreover, because cash withdrawals are limited to $500 per branch per day, Tanzman sometimes travels to multiple Patelco branch offices in a given day to withdraw sufficient cash. He spends significant time each day (at least an hour) simply travelling to and from Patelco branches. Tanzman also needed to acquire a cashier's check as payment to move into a new rental apartment but could not do so because Patelco's services were offline as a result of the Data Breach. He has concerns for his personal financial security as a result of the Data Breach.

67. In addition, Tanzman is disabled and is currently living with disabling HIV/AIDS. Because of his weakened immune system, he has been advised by his doctor to avoid unnecessary public interactions. He thus relies on Patelco's mobile app and online banking system to manage his finances. Because those systems were offline due to the Data Breach, causing Tanzman to visit Patelco branches to withdraw funds, the Breach exposed him to serious risks to his health. It also caused Tanzman extreme stress, which may further exacerbate his condition. In one recent visit to a Patelco

branch office in San Francisco following the Data Breach, Tanzman experienced a violent encounter, in which an unidentified man threatened to attack him with a knife. But for the Data Breach, and Tanzman's resulting need to visit branch offices in person, this incident would not have occurred.

68. Van Antwerp and Tanzman suffered actual injuries in the form of damages to and diminution in the value of his PII—a form of intangible property was entrusted to Defendant—which was compromised as a proximate result of the Data Breach.

69. Van Antwerp and Tanzman have also experienced severe financial and emotional stress as a result of the Data Breach. They have experienced significant distress following the Data Breach given Defendant's conduct at issue, the sensitive nature of their stolen PII, and Defendant's failure to identify which of their information was compromised. This goes beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

70. Van Antwerp and Tanzman will spend time protecting themselves from identity theft resulting from the Data Breach for the foreseeable future and beyond. They will suffer imminent and impending injuries arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from their PII being obtained by cybercriminals.

71. Van Antwerp and Tanzman have a continuing interest in ensuring that their PII, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches or cybersecurity risks.

72. Defendant deprived Van Antwerp and Tanzman of the earliest opportunity to guard themselves against the Data Breach's harmful effects by failing to adequately notify them about it.

73. Had Van Antwerp and Tanzman known about Defendant's lax data security, they would not have provided their PII to Defendant.

### F. Plaintiffs and the Class Suffered Actual and Impending Injuries Resulting from the Data Breach

74. As a proximate result of Defendant's unreasonable security practices, identity thieves now possess the sensitive PII of Plaintiffs and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to Plaintiffs and the Class. On the dark web—an

underground Internet black market—criminals openly buy and sell stolen PII to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts, and credit cards, file false insurance claims or tax returns, or rack up other kinds of expenses.[27] And, "[t]he damage to affected [persons] may never be undone."[28]

75. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[29] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[30]

76. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit

[27] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (Jun. 7, 2021), FORBES, https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=ca928c05650d.

[28] *Id.*

[29] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Oct. 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[30] *Id.*

> cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.
>
> Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[31]

77. Even when an injured person successfully goes through the cumbersome and time-consuming process of changing their Social Security number following identity theft, the Social Security Administration cautions individuals to "[k]eep in mind that a new number probably won't solve all your problems" and "can't guarantee you a fresh start."[32]

78. Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

79. Defendant's data breach notices to affected persons do not provide adequate remediation and compensation for its wrongful conduct and actions described herein.

## CLASS ACTION ALLEGATIONS

80. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> **All persons whose PII was compromised in the Data Breach disclosed by Patelco Credit Union on June 29, 2024.**

81. Within the Nationwide Class, there is one California Subclass defined as follows:

[31] Identity Theft and Your Social Security Number, U.S. SOCIAL SECURITY ADMINISTRATION (JULY 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.

[32] *Id.*

**All persons in the State of California whose PII was compromised in the Data Breach disclosed by Patelco Credit Union on June 29, 2024.**

82. Excluded from the Nationwide Class and Subclass are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and Subclass are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

83. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

84. ***Numerosity Under Rule 23(a)(1).*** The Nationwide Class and Subclass are so numerous that the individual joinder of all members is impracticable, and the disposition of the claims of all members of the Nationwide Class and Subclass in a single action will provide substantial benefits to the parties and the Court. Although the precise number of members of the Nationwide Class and Subclass are unknown to Plaintiffs at this time, on information and belief, the proposed Nationwide Class contains at least 450,000 individuals, and the proposed Subclass contains at least hundreds of thousands of individuals. Discovery will reveal, through Defendant's records, the number of members of the Nationwide Class and Subclass.

85. ***Commonality Under Rule 23(a)(2).*** Common legal and factual questions exist that predominate over any questions affecting only individual members of the Nationwide Class and Subclass. These common questions, which do not vary among members of the Nationwide Class or the Subclass and which may be determined without reference to any Nationwide Class or Subclass Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that its computer systems and networks were vulnerable to unauthorized third-party access or a cyberattack;

b. Whether Defendant failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that its computer systems and networks were protected;

c. Whether Defendant failed to take available steps to prevent and stop the Data Breach from occurring;

d. Whether Defendant owed a legal duty to Plaintiffs and Class Members to protect their PII;

e. Whether Defendant breached any duty to protect the PII of Plaintiffs and Class Members by failing to exercise due care in protecting their sensitive and private information;

f. Whether Defendant provided timely, accurate, and sufficient notice of the Data Breach to Plaintiffs and the Class Members;

g. Whether Plaintiffs and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

h. Whether Plaintiffs and Class Members are entitled to injunctive or equitable relief, including restitution.

86. ***Typicality Under Rule 23(a)(3).*** Plaintiffs' claims are typical of the claims of the Nationwide Class and Subclass. Plaintiffs, like all proposed members of the Class and Subclass, had their PII compromised in the Data Breach. Defendant's uniformly unlawful course of conduct injured Plaintiffs and Class Members in the same wrongful acts and practices. Likewise, Plaintiffs and other Class Members must prove the same facts in order to establish the same claims.

87. ***Adequacy of Representation Under Rule 23(a)(4).*** Plaintiffs are adequate representatives of the Nationwide Class and Subclass because they are Class and Subclass Members, and their interests do not conflict with the interests of the Nationwide Class or Subclass. Plaintiffs have retained counsel competent and experienced in complex litigation and consumer protection class action matters such as this action, and Plaintiffs and their counsel intend to vigorously prosecute this action for the Nationwide Class's and Subclass's benefit and have the resources to do so. Plaintiffs and their counsel have no interests adverse to those of the other members of the Class or Subclass.

88. ***Predominance and Superiority.*** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of each Nationwide Class and Subclass Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Nationwide Class and Subclass will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Even if each Nationwide Class and Subclass Member could afford

individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

89. As a result of the foregoing, class treatment under Fed. R. Civ. P. 23(b)(2) and (b)(3) is appropriate.

## FIRST CAUSE OF ACTION
**Negligence**
***(On Behalf of Plaintiffs and the Nationwide Class)***

90. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

91. In the course of providing services, Defendant solicited, gathered, and stored the PII of Plaintiffs and Class Members. Because Defendant was entrusted with such PII at all relevant times, Defendant owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to its networks and systems. This duty arose independently from any contract.

92. Defendant knew, or should have known, of the risks inherent in collecting and storing massive amounts of PII, including the importance of adequate data security and the high frequency of ransomware attacks and well-publicized data breaches both generally and the increasing rate of cybercriminals specifically targeting the financial services industry. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security

would result in the compromise of that sensitive information. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII by failing to limit access to this information to unauthorized third parties and by not properly supervising both the way the PII was stored, used, and exchanged, and those in its employ responsible for such tasks.

93. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII . Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

94. Defendant also had a common law duty to prevent foreseeable harm to others. Defendant had full knowledge of the sensitivity and high value of the PII that it stored and the types of foreseeable harm and injury-in-fact that Plaintiffs and Class Members could and would suffer if that PII were wrongfully disclosed, leaked, accessed, or exfiltrated. Defendant's conduct created a foreseeable and unreasonable risk of harm to Plaintiffs and Class Members, who were the foreseeable victims of Defendant's inadequate data security practices.

95. Defendant violated its duty to implement and maintain reasonable security procedures and practices, including through its failure to adequately restrict access to its file share systems that held hundreds of thousands of individuals' PII or encrypt or anonymize such data. Defendant's duty included, among other things, designing, maintaining, and testing Defendant's information security controls to ensure that PII in its possession was adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

96. Defendant's duty of care also arose by operation of statute. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiffs and Class Members. The FTC Act was enacted to protect Plaintiffs and the Class Members from the type of conduct in which Defendant engaged.

97. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' PII.

98. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII no longer necessary for its provision of services, allowing unmonitored and unrestricted access to unsecured PII, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Members' confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act.

99. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members. Timely disclosure was necessary so that Plaintiffs and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; and (vi) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

100. Defendant had the financial and personnel resources necessary to prevent the Data Breach. Defendant nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiffs and Class Members.

101. Plaintiffs and Class Members had no ability to protect their PII once it was in Defendant's possession and control. Defendant was in an exclusive position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

102. But for Defendant's breach of its duty to adequately protect Class Members' PII, Class Members' PII would not have been stolen. As a result of Defendant's negligence, Plaintiffs and Class Members suffered and will continue to suffer the various types of damages alleged herein. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

103. As a direct and traceable result of Defendant's negligence, Plaintiffs and the Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiffs and the Class include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendant; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (vi) unauthorized use of compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in its possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

104. Defendant's negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendant's care, and its failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

105. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

## SECOND CAUSE OF ACTION
**Invasion of Privacy**
***(On Behalf of Plaintiffs and the Nationwide Class)***

106. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

107. Plaintiffs and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

108. Plaintiffs and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their private information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

109. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class Members by engaging in the conduct described above, including by failing to protect their PII by permitting unauthorized third parties to access, exfiltrate, and view this private information. Likewise, Defendant further invaded the privacy rights of Plaintiffs and Class Members, and permitted cybercriminals to invade the privacy rights of Plaintiffs and Class Members, by unreasonably and intentionally adequate delaying disclosure of the Data Breach and failing to properly identify what PII had been accessed, exfiltrated, and viewed by unauthorized third-parties.

110. This invasion of privacy resulted from Defendant's failure to properly secure and maintain Plaintiffs' and the Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

111. Plaintiffs' and the Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and the Class Members' PII, and such private information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

112. The disclosure of Plaintiffs' and the Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

113. Defendant's willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and the Class Members' sensitive PII is such that it would cause serious mental injury, shame, embarrassment, or humiliation to people of ordinary sensibilities.

114. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and the Class Members' PII was without their consent, and in violation of various statutes, regulations, and other laws.

115. As a result of the invasion of privacy caused by Defendant, Plaintiffs and the Class Members suffered and will continue to suffer damages and injury as set forth herein.

116. Plaintiffs and the Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

## THIRD CAUSE OF ACTION
**Unjust Enrichment / Quasi-Contract**
***(On Behalf of Plaintiffs and the Nationwide Class)***

117. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

118. A monetary benefit was conferred upon Defendant through its receipt of Plaintiffs' and Class Members' PII, which Defendant used to facilitate its services. Defendant appreciated or had knowledge of these benefits conferred upon it by Plaintiffs and the Class.

119. Under principles of equity and good conscience, Defendant should not be permitted to retain the full monetary value of the benefit because Defendant failed to adequately protect Plaintiffs' and Class Members' PII.

120. Plaintiffs and the Class Members have no adequate remedy at law. Defendant continues to retain their PII while exposing this sensitive and private information to a risk of future data breaches while in Defendant's possession. Defendant also continues to derive a financial benefit from using Plaintiffs' and Class Members' PII.

121. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class Members have suffered various types of damages alleged herein.

122. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it because of its misconduct described herein and the Data Breach.

## FOURTH CAUSE OF ACTION
**California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100, *et seq.***
***(On Behalf of Plaintiffs and the California Subclass)***

123. Plaintiffs, individually and on behalf of the Subclass, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

124. The California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100, *et seq.* ("CCPA"), was enacted to protect individuals' PII from collection and use by businesses without appropriate notice and consent.

125. Through the conduct and actions complained of herein, Defendant violated the CCPA by subjecting Plaintiffs and California Subclass Members' nonencrypted PII to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duties to implement and

maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Defendant thereby violated CAL. CIV. CODE § 1798.150(a).

126. As a direct and proximate result of Defendant's acts, Plaintiffs and the California Subclass's PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer networks, servers, and systems.

127. As a direct and proximate result of Defendant's acts, Plaintiffs and the California Subclass were injured and lost money or property, including but not limited to the loss of the California Subclass's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

128. Defendant knew or should have known that its computer systems, servers, and networks and data security practices were inadequate to safeguard the California Subclass's PII and that the risk of a serious data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and the California Subclass.

129. Plaintiffs and the California Subclass Members are "consumers" within the meaning of CAL. CIV. CODE § 1798.140(i) because they are California residents.

130. Defendant collected Plaintiffs and the California Subclass's "personal information" within the meaning of CAL. CIV. CODE §§ 1798.140(v) and 1798.80(e).

131. Defendant is a limited liability partnership organized or operated for the profit or financial benefit of their owners, partners, and other shareholders. Defendant "collected" Plaintiffs and the California Subclass's "personal information" within the meaning of CAL. CIV. CODE § 1798.140(v). Defendant does business in the State of California and has annual gross revenues exceeding $25 million. Accordingly, Defendant is a "business" within the meaning of the CAL. CIV. CODE § 1798.140(d) and is obligated to comply with the CCPA's requirements.

132. Pursuant to CAL. CIV. CODE § 1798.150(b), counsel for Plaintiffs will serve Defendant with notice of these CCPA violations by certified mail, return receipt requested.

133. On behalf of California Subclass Members, Plaintiffs presently seek actual pecuniary damages and injunctive relief in the form of an order enjoining Defendant from continuing to violate

the CCPA. Unless and until Defendant is restrained by order of the Court, its wrongful conduct will continue to cause irreparable injury to Plaintiffs and the California Subclass.

134. If Defendant fails to timely rectify or otherwise cure the CCPA violations described herein, individually and on behalf of the California Subclass, Plaintiffs reserve their right to amend this Class Action Complaint to seek statutory damages and any other relief the Court deems proper as a result of Defendant's CCPA violations pursuant to CAL. CIV. CODE § 1798.150(a).

## FIFTH CAUSE OF ACTION
**California Customer Records Act, CAL. CIV. CODE §§ 1798.80, *et seq.***
***(On Behalf of Plaintiffs and the California Subclass)***

135. Plaintiffs, individually and on behalf of the Subclass, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

136. "[T]o ensure that personal information about California residents is protected," the California legislature enacted CAL. CIV. CODE § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

137. Defendant is a business that owns, maintains, or licenses personal information, within the meaning of CAL. CIV. CODE § 1798.81.5, about Plaintiffs and California Subclass members.

138. Defendant violated CAL. CIV. CODE § 1798.81.5 by failing to implement reasonable measures to protect California Subclass members' PII.

139. Businesses that own or license computerized data that includes personal information are required to notify California residents when their PII has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." CAL. CIV. CODE § 1798.82. Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach." CAL. CIV. CODE § 1798.82.

140. Defendant is a business that owns or licenses computerized data that includes personal information as defined by CAL. CIV. CODE § 1798.82.

141. Plaintiffs and California Subclass Members' PII includes personal information identified in CAL. CIV. CODE § 1798.82(h) such as their names, Social Security numbers, driver's license numbers, and financial information, and is thereby covered by CAL. CIV. CODE § 1798.82.

142. Plaintiffs and the California Subclass Members are "customers" within the meaning of CAL. CIV. CODE § 1798.80(c), as their personal information was provided to Defendant for the purpose of obtaining services or products.

143. The Data Breach constituted a breach of Defendant's security systems, networks, and servers.

144. Because Defendant reasonably believed that Plaintiffs and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by CAL. CIV. CODE § 1798.82.

145. Defendant unreasonably delayed informing Plaintiffs and the California Subclass Members about the breach of security of their PII after it knew the breach had occurred.

146. Upon information and belief, no law enforcement agency instructed Defendant that notification to California Subclass Members would impede an investigation.

147. Thus, by failing to disclose the Data Breach in a timely and accurate manner, the Defendant also violated CAL. CIV. CODE § 1798.82.

148. Pursuant to CAL. CIV. CODE § 1798.84, "[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable," "[a]ny customer injured by a violation of this title may institute a civil action to recover damages," and "[a]ny business that violates, proposed to violate, or has violated this title may be enjoined."

149. As a direct and proximate result of Defendant's violations of CAL. CIV. CODE §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members were (and continue to be) injured and suffered (and will continue to suffer) damages, as described above.

150. Plaintiffs and California Subclass Members seek relief under CAL. CIV. CODE § 1798.84, including, but not limited to, actual damages, any applicable statutory damages, and equitable and injunctive relief.

## SIXTH CAUSE OF ACTION
**California Unfair Competition Law, CAL. BUS. & PROF. CODE §§ 17200, *et seq.***
***(On Behalf of Plaintiffs and the California Subclass)***

151. Plaintiffs, individually and on behalf of the Subclass, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

152. Defendant violated California's Unfair Competition Law (the "UCL"), CAL. BUS. & PROF. CODE §§ 17200, *et seq.*, by engaging in unlawful, unfair, or fraudulent business acts and practices that constitute acts of "unfair competition" as defined in the UCL with respect to its conduct and actions with towards Plaintiffs and the California Subclass.

153. Defendant's actions as alleged herein in this Class Action Complaint constitute an "unlawful" practice as encompassed by CAL. BUS. & PROF. CODE §§ 17200, *et seq.* because Defendant's actions: (a) violated the California Consumer Records Act, CAL. CIV. CODE §§ 1798.80, *et seq.*, (b) violated the CCPA, CAL. CIV. CODE §§ 1798.100, *et seq.*, (c) constituted negligence; and (d) violated federal law and regulations, including the FTC Act.

154. Defendant's actions as alleged in this Class Action Complaint also constitute an "unfair" practice as encompassed by CAL. BUS. & PROF. CODE §§ 17200 *et seq.*, because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious. The harm caused by Defendant's wrongful conduct outweighs any utility of such conduct and has caused—and will continue to cause—substantial injury to the California Subclass. There were ample reasonably available alternatives that would have furthered Defendant's legitimate business practices, including using industry-standard technologies to protect data (e.g., two-factor authorization, effective encryption and anonymization, software patches, and the purging of data no longer necessary for Defendant's services). Defendant also unreasonably delayed in notifying Plaintiffs and the California Subclass Members regarding the unauthorized release and disclosure of their PII. Additionally, Defendant's conduct was "unfair" because it violated the legislatively declared policies reflected by California's strong data-breach and online-privacy laws, including the California

Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, the CCPA, Cal. Civ. Code §§ 1798.100, *et seq.*, and the California constitutional right to privacy, CAL. CONST. ART. 1, § 1.

155. As a result of Defendant's unlawful and unfair conduct, Plaintiffs and the California Subclass were damaged and injured by the significant costs of protecting themselves from identity theft and face ongoing and impending damages related to theft of their PII.

156. Defendant's wrongful practices constitute a continuing course of unfair competition because, on information and belief, Defendant has failed to remedy the lax security practices or even fully notify all affected California persons. Plaintiffs and the California Subclass seek equitable relief pursuant to Cal. Bus. & Prof. Code § 17203 to end Defendant's wrongful practices and require Defendant to maintain adequate and reasonable security measures to protect the PII of Plaintiffs and the California Subclass.

157. Plaintiffs and California Subclass Members lack an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages, as well as long term incalculable risk associated with medical fraud.

158. Further, if an injunction is not issued, Plaintiffs and California Subclass Members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Defendant has still not provided adequate information on the cause and scope of the Data Breach. Plaintiffs and California Subclass Members lack an adequate remedy at law that will reasonably protect against the risk of a further breach.

159. Plaintiffs and the California Subclass also seek an order requiring Defendant to make full restitution of all monies it received through its wrongful conduct, along with all other relief permitted under Cal. Bus. & Prof. Code §§ 17200, *et seq.*

## SEVNENTH CAUSE OF ACTION
**Injunctive/Declaratory Relief**
***(On Behalf of Plaintiffs and the Nationwide Class)***

160. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

161. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

162. Defendant owes a duty of care to Plaintiffs and Class Members, which required Defendant to adequately monitor and safeguard Plaintiffs' and Class Members' PII.

163. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII belonging to Plaintiffs and Class Members.

164. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their private information will occur in the future.

165. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiffs and the Class within its care, custody, and control under the common law and Section 5 of FTC Act;

b. Defendant breached its duty to Plaintiffs and the Class by allowing the Data Breach to occur;

c. Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII of Plaintiffs and the Class within Defendant's custody, care, and control; and

d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiffs and the Class.

166. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect the PII of Plaintiffs and the Class within its custody, care, and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems, networks, and servers on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII within its servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendant to provide adequate services;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

167. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is

real, immediate, and substantial. If another data breach or cybersecurity incident occurs, Plaintiffs and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiffs and the Class for the serious risks of future harm.

168. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a preexisting legal obligation to employ such measures.

169. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident, thus preventing future injury to Plaintiffs and the Class and other persons whose PII would be further compromised.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. Certifying this action as a class action under Fed. R. Civ. P. 23 and appointing Plaintiffs and their counsel to represent the Class and Subclass;

B. Entering judgment for Plaintiffs, the Class, and the Subclass;

C. Granting permanent and appropriate injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII of Plaintiffs and the Class by implementing improved security controls;

D. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

E. Award statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;

F. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

G. Awarding to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

I. Granting such further and other relief as may be just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a jury trial on all claims so triable.

Dated: July 14, 2024

*/s/ Amber L. Schubert*

Robert C. Schubert (No. 62684)
Amber L. Schubert (No. 278696)
**SCHUBERT JONCKHEER & KOLBE LLP**
2001 Union. St., Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

*Counsel for Plaintiffs*